An Overview of Information Operations in the Indian Army

By Sapan Kumar Chatterji, Brigadier General, Indian Army

***Editorial Abstract:** Brigadier General Chatterji believes India's IO methods differ only slightly from those used by many Western nations. Such distinctions include methods such as economic information warfare, in which one nation could strangle another's access to external data, thereby removing the benefits associated with exchange of information and thereby crippling the economy. He believes India has other independent initiatives that have expanded the overall meaning and use of IO, including the topic of sub conventional operations.*

Information operations (IO), as a concept, are as old as man's quest for warfare and his dependence on information. However, its role has increased tremendously due to the exceptional growth in technology over the past few decades. Indian mythology circa 5000 BC is replete with examples of the innovative and effective use of information warfare as a war winning effort. The announcement of the death of Ashwathama amidst the beating of drums (jamming), and various other tactics of Lord Krishna to gain information superiority, are just a few of the numerous epic examples.

Today, the importance of IO during recent conflicts and the ongoing counter-terrorism operations in Jammu & Kashmir [Indian provinces] have undisputedly created a new dimension of battle. IO has become the fifth dimension of warfare. This article covers the concept of information warfare in the Indian Army, as well as certain counterinsurgency initiatives India has taken in the past few years. The discussion covers: the objective and principles of information warfare; the terminology of information warfare; the forms of IW; the necessity to deny use of the Internet to terrorists; and the role of information warfare in sub-conventional operations.

Objectives/Principles of IW

IW is utilized to achieve all or any of the following objectives:

• Develop and maintain a comprehensive information base of an adversary's capabilities, and forecast their likely actions.

• Deny information about one's own and other friendly forces, and deny information about operations conducted against enemies and adversaries.

• Influence perceptions, plans, actions, and the will of adversaries to oppose our own/friendly forces by the use of offensive IW.

• Influence noncombatant and neutral organizations to support friendly missions, or at least not resist friendly activities.

• Protect friendly decision making processes, information, and information systems.

• Degrade adversaries' information systems.

IW is the result of competition brought about by the convergence of a number of evolving technologies, including imaging, remote sensing, precision guided munitions, stealth, directed energy weapons, and above all digital communications & computer networks. During conflict, these technologies are in direct confrontation.

Terminology

Terms used here include:

• Information Operation (IO) - Actions taken to affect adversary information and information systems, while defending one's own information and information systems;

• Information warfare (IW) - Action taken during all forms of conflict, to achieve information superiority over the adversary by adversely affecting his information and information systems while protecting one's own information and information systems;

• Information Assurance - Information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing protection, detection, and reaction capabilities;

• Information Superiority - A state achieved when a competitive advantage is derived from the ability to exploit a superior information position.

Forms of IW

IW is not a distinct type of warfare but exists in different forms. IW can be applied at every level of war, across all phases of an operation, and encompasses the entire range of military operations. The Indian Army defines seven forms of IW:

• Command & Control Warfare (C2W)
• Electronic Warfare (EW)
• Cyber Warfare (Cyber W)
• Network Centric Warfare (NCW)
• Intelligence Based Warfare (IBW)
• Psychological Warfare (PSYWAR)
• Economic Information Warfare (EIW)

C2W

C2W implements information warfare on the battlefield, and integrates it with physical destruction. Its objective is to decapitate the enemy's command structure from the body of forces. C2W aims to influence, deny information, degrade, or destroy enemy C2 capabilities, while protecting one's own C2 systems against such actions. C2W is the war fighting application of IW in military operations.

The foundation of C2W lies in efficient command, control, communications, and computer (C4) systems, coupled with seamless information and intelligence support. C2W consists of the following:

• OPSEC - A process of identifying critical information and one's own actions that can be observed by enemy intelligence systems, determining indicators an enemy could interpret to derive critical information on one's own forces; and selecting and executing measures that eliminate the vulnerabilities of one's actions to enemy exploitation;

• Military Deception - Actions executed to mislead enemy commanders as to one's capabilities, intentions, and operations;

• Psychological Operations - The purpose of PSYOP is to induce enemy attitudes and behavior favorably to one's objectives;

• EW - Military action involving the use of the electromagnetic and directed energy spectrums in order to control the electromagnetic spectrum;

• Physical Destruction - The application of combat power to destroy or neutralize hostile C2 targets.

EW

EW is a set of military actions taken to deny the use of the electromagnetic spectrum to hostile forces while retaining the ability to use it. The endeavor is to deny, degrade, delay, or disrupt information in order to create a false picture so that incorrect action results. Major components of EW :

• Electronic Support Measures (ESM)

• Electronic Counter Measures (ECM)

• Electronic Counter-Counter Measures (ECCM)

Cyber Warfare

Cyber warfare entails techniques to destroy, degrade, exploit, or compromise the enemy's computer based systems—including attacks on computer networks. In contrast to physical combat, these attacks exploit known lapses in a systems security structure. Cyber warfare includes the following actions:

• Techniques to destroy, degrade, exploit, or compromise the enemy's computer based systems;

• Attacks on computer networks;

• Hacking/breaking into computer networks to include defacing websites;

• Intercepting and monitoring classified information on networks, corrupting and manipulating stored data, and injecting viruses likely to cause irreparable losses;

• Cyber security, including encryption.

Network Centric Warfare (NCW)

NCW focuses on the combat power that can be generated from the effective linking or networking of war fighting machinery/organizations. The basic elements necessary to generate the required shared battle space awareness to achieve the Commander's intent are:

Indian soldiers raise their national colors. (MOD India)

• A virtual sensor or "surveillance" grid that would provide a "grid of capabilities" overlaying the battle space instead of a series of independent single sensors;

• A communications grid that would leverage the strength of the worldwide telecommunications infrastructure. This would enable communications to be considered as virtual grids overlaying the tactical, operational, and strategic areas;

•An abstract grid of weapons or "tactical grid" available to commanders, sorted by suitability and availability against a hostile order of battle.

Intelligence Based Warfare (IBW)

IBW occurs when intelligence is fed directly into operations, instead of being used as input for overall command and control. As sensors grow more accurate and reliable, proliferate in type and number, and as they become capable of feeding fire control systems in real-time and near-real-time, the task of developing, maintaining, and exploiting systems that sense the battlefield, assess its composition, and send results to shooters assumes greater importance for tomorrows militaries.

IBW is about conducting warfare in a transparent battlefield environment. However, while increasing the transparency for one's own functioning, an important consideration should be to decrease it for the enemy. The need is to create an asymmetry in the level of transparency or situational awareness, in relation to the enemy.

Psychological Warfare

Psychological Warfare encompasses the use of information to influence the human mind. It is also defined as actions carried out during peace, crisis, or wartime situations, so as to influence the attitudes and behavior of enemy, friendly, or neutral audiences, towards fulfillment of political and military objectives.

Psychological operations can be used over the entire support spectrum of military operations, wherein all agencies work in synergy to achieve the desired end state. The aims of psychological operations from a military point of view are:

• Create of doubt, dissidence, and dissatisfaction within the ranks and thereby lowering the morale and reducing the efficiency of adversary forces;

• Reinforce the feeling of friendly target audiences and influence opinion makers;

• Gain support and cooperation of uncommitted or undecided audiences;

• Help achieve conflict prevention, resolution, and achieve a desired end state.

Psychological operations are divided into four distinct but overlapping categories:

• Strategic Psychological Operations - This is PSYOP at the national level, conducted predominately outside the military arena. It utilizes all national assets and is directed at all types of audiences. Objectives are long term. The primary aim is to reduce the war making capability of the adversary;

• Operational Psychological Operations - This type is conducted during both war and peace time in the operational area to promote the operational commanders aims and objectives. These operations are launched in consonance with military operations, throughout the military operational area. All assets in the operational area are utilized;

• Tactical Psychological Operations - These are conducted in the tactical arena, in consonance with tactical missions and objectives;

• Counter Psychological Operations - The aim of this type of PSYOP is to safeguard one's own forces and friendly population from an adversary's psychological operations. One must simultaneously carry out counter psychological operations, identifying an adversary's broad pattern of operations, to include the technical means and medium of dissemination. Countermeasures are then instituted, including informing the audience about the adversary's malicious agenda.

The most popular non-military and military mediums used for the dissemination of psychological operations are print, television, radio, and cyber. Print is one of the most effective and widely used media, which has been used extensively in all psychological campaigns to target educated target audiences. Newspaper, magazines, leaflets, posters, pamphlets, and books are associated with this medium.

Television, with its ever-increasing popularity, is one of the most powerful, flexible, and immediate means of influence. It has become a very important psychological tool, as effectively demonstrated during the Gulf Wars and the 1999 Kargil operations. Television was an extensive part of the psychological campaign, and instrumental in achieving the final military objective.

Radio has been used as an important psychological operations tool since World War I, due to its reach and capability to affect target audiences. It can penetrate inaccessible areas to target insurgents, enemy soldiers, and at the same time help in the psychological conditioning of one's own forces.

Finally, there is the cyber dimension. The Internet has become a very important media tool. The numbers of Internet users are increasing rapidly, and in time will be one of the most powerful means of dissemination for one's own psychological operations. At the same time, this medium is also available to adversaries and terrorists, hence there is a need to monitor and counter malicious propaganda.

Indian Armed Forces Emblem (Wikipedia.org)

Economic Information Warfare

This form of warfare is only conducted at the national level, as a combination of IW and economic warfare. It can also be understood as a variant of an economic blockade, wherein the well being of societies will be affected by information flows of economic data, instead of the flow of material supplies as they are today. In this form of warfare nations would strangle another nation's access to external data, removing the benefits associated with the exchange of information, and thereby crippling the economy. Nations would also struggle with one another to dominate strategic economic industries.

Denying the Internet to Terrorists

With terrorists using cyberspace to communicate and coordinate their activities, denying them this medium is certainly an important issue. However, there are a large number of factors that impede nations from undertaking serious and immediate steps, since these could easily violate individual privacy—and affect the performance of knowledge-based industries.

Monitoring of Data

It is impossible to monitor every byte transaction on the Internet because the volumes are simply too huge. Unless explicitly warranted, democracies should not resort to monitoring. However, most nations need to consider or implement selective monitoring. This is achievable through liaising with Internet service providers on explicit state orders. Such monitoring can be done at gateways and routers, or the "last mile" stubs (i.e. switches / routers) where specific intelligence is available.

Who to monitor, where to filter, or which switch/router to monitor can only be determined through hard intelligence. Therefore, it is extremely important to establish coordination between various intelligence agencies for this specific purpose. Methods include using certain keywords for the purpose of filtering/ identifying intelligence data.

Cyberspace monitoring can reap rich dividends if a state obtains hard intelligence. Further, the threat arising from cyberspace needs analysis and planning. For this purpose, Risk Mitigation Plan / Disaster Recovery Plan (DRP) development are the best recommendations. At the national level such a contingency plan helps ensure that should critical resources be damaged, emergency measures and services are in place. India needs to put the DRP in action, and exercise it periodically.

Cyber Laws Dealing with Mail / Blog / Portal Service Providers

Communications between terrorists would usually take place through standard mail portals, chat rooms, etc. States need laws need to enact and duly amalgamate international laws, to provide understanding and cooperation, so that should a nation request transaction details or trace back details for any user, ISPs will provide answers. Such actions must be transparent through international boundaries, based on the need to fight this menace jointly at the international level. In addition, since terrorists use the Internet for recruitment through misinformation, some of the steps we could take in this direction are:

• Exchange information pertaining to websites, blogs, chat rooms, etc. between nations that might contain offensive material;

• Block such websites in our national interest;

• Host websites (as a part of Psychological Operations) containing actual, factual information that might be used to influence, and sway away potential targets, or from embracing terror activities;

• Track down offensive websites and close them if hosted in our countries.

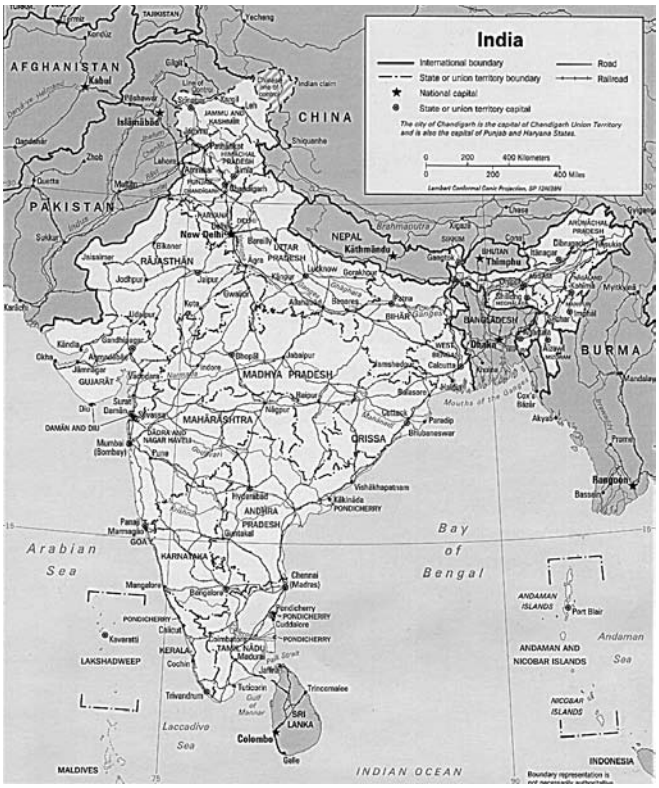
An international treaty of this kind, enacted and enforced, can help ensure we deny terrorists space for hosting such sites.

Cyber Policing

To detect and annihilate the terrorists' Internet attack planning and coordinating medium, we need to develop Cyber Policing Organizations. Hard intelligence must be gathered from cyberspace to provide enough clues to allow for the tracking of criminals and terrorists. The capabilities to handle multiple protocols, encrypted algorithms, code breaking, and so on should be incorporated into our monitoring agencies.

Building a Cyber Forensic Capability

India needs to establish a Network Cyber Forensic capability to enable trace back of messages, attacks, and other malicious activities. The international community needs to develop IT laws that support state sponsored cyber forensics, not only for the purpose of tracking down terrorists, but for use as legal exhibits in a court of law. PC-based forensics designed for data recovery can help to wean out intelligence captured from terrorists. Similarly, India needs to compile a cryptology analysis capability, so we can crack encrypted traffic and break passwords. This requires long term government-sponsored initiatives, say at academic institutes or at research institutions. However, this too is a expensive and longer range activity.



India in its south Asian context. (Wikimedia)

Sub Conventional Operations

Sub conventional warfare is a generic term encompassing all armed conflicts above the level of peaceful coexistence amongst states, and below the threshold of war. This includes militancy, insurgency, proxy war, and terrorism when employed as a means in an insurrectionist movement, or undertaken independently. Border skirmishes also fall within this category. Sub conventional warfare entails protracted struggle. It could also be characterized by asymmetry of force levels between regular forces and irregulars, wherein the force applied and the violence generated depends on the modus operandi of the weaker side—and the laws of the land which bind the actions of the Armed Forces. For this discussion we'll consider counterterrorist operations, and public information and perception building operations.

Counter Terrorist Operations

Information operations in the context of the sub conventional spectrum address the following:

• Countering adverse effects of counterterrorist (CT) operations;

• Supporting the goals and operations of one's own forces;

• Defeating malicious propaganda;

• Eroding the terrorists' support base;

• Helping justify one's own operations and projecting the "human face" of the Armed forces

• Winning the hearts and minds (WHAM) of the local population, thereby lessening popular support for terrorist causes;

• Publicizing incentives to the local people in return for information on terrorist activities;

• Persuading terrorists about the futility of their goals against one's own military might.

Military Civic Action

Military Civic Actions (MCA) include programs such as WHAM activities aimed at people in insurgency affected areas, as part of the strategy for conflict prevention. WHAM operations form a major concomitant aspect of counterinsurgency operations. They are integral to the Army's psychological strategy as well. Civic actions include a wide range of activities, across the entire spectrum of development, and demonstrate the Army's "human face." The focus of WHAM operations are quality education, empowerment of women, community development, health care, and infrastructure improvement.

There are several elements associated with the MCA concept. The "iron fist with a velvet glove" concept involves relentless operations, undertaken with a firm resolve against foreign terrorists, and at the same time encouraging terrorists to surrender. These are intelligence driven surgical operations. In addition, forces adopt a people friendly approach, aiming to 'win hearts and minds' and to project the Army's image as "people with a human face." WHAM projects are usually small scale, but generally appreciated, afforded maximum visibility, and very popular.

A second element associated with MCA operations involves centralized planning and decentralized execution. Countries identify civic action projects in consultation with local community leaders, administration, and execution agencies. The plans evolve following a top down (priorities, broad allocation of resources) and bottom up (identification of projects and resource bids) approach. The focus of the projects at the village level is on women and youth. The maximum use of indigenous labor—both skilled and unskilled—goes a long way toward dissuading youths from joining the ranks of terrorists.

Other elements involve providing assistance in the planning and extension of technical assistance, and providing material resources and supervision. When the projects are completed, they are handed over to the civil administration/village councils for operations, maintenance, and upkeep.

The focus of WHAM activities in an insurgency prone area includes:

• Causality Evacuation and Rehabilitation during Natural Calamities

• Vocational Training

• Health Care

• Community Development

• Infrastructure Development

• Education Facilities

Public Information and Perception Building Operations

Public Information Operations to influence perceptions of various players in the conflict zone should be undertaken in accordance with developed themes. At the operational level, these themes could be:

• The futility of the armed struggle and secessionist designs;

• The efforts of the government regarding relief and rehabilitation schemes to restore normalcy;

• The erosion of the credibility of terrorists and secessionist elements;

• The importance and efficacy of one's own operations;

• A people friendly Army approach and its efforts to alleviate suffering that was caused by the terrorists;

• The importance of peace for the overall prosperity of the people and details of the government's peace initiatives.

Conclusion

This article has attempted to briefly provide insight as to how India understands information operations, as well as certain of our own initiatives for directing the future of IO. Overall, India's doctrine and methods differ only slightly from those used by many Western nations. With regard to certain independent initiatives that have expanded the overall meaning and use of IO, our nation adds the topic of sub conventional operations as but one example.

Today, information is one of the most powerful tools available to nations during a conflict. The nation that attains information superiority stands to gain immensely. Nations who work together toward common information goals stand to gain the most.